Fecha de presentación: octubre, 2021, **Fecha de Aceptación**: diciembre, 2021, **Fecha de publicación**: enero, 2022

24

USO DE LAS CONTRASEÑAS ENTRE LOS ESTUDIANTES UNIVERSITARIOS. EL CASO DE UNA UNIVERSIDAD PÚBLICA MEXICANA

PASSWORDS USE AMONG UNIVERSITY STUDENTS. THE CASE OF A MEXICAN PUBLIC UNIVERSITY

Ramón Ventura Roque Hernández[1]
E-mail: rvhernandez@uat.edu.mx
ORCID: https://orcid.org/0000-0001-9727-2608
René Adrián Salinas Salinas[1]
E-mail: srene@docentes.uat.edu.mx
ORCID: https://orcid.org/0000-0001-5464-4707
Dante Rodríguez Cordero[1]
E-mail: drodriguez@uat.edu.mx
ORCID: https://orcid.org/0000-0001-8316-7831
Mario Alberto Villarreal Álvarez[1]
E-mail: valvarez@docentes.uat.edu.mx
ORCID: https://orcid.org/0000-0003-0605-7633
[1]Universidad Autónoma de Tamaulipas. México.

Cita sugerida (APA, séptima edición)

Roque Hernández, R. V., Salinas Salinas, R. A., Rodríguez Cordero, D., & Villarreal Álvarez, M. A. (2022). Uso de las contraseñas entre los estudiantes universitarios. El caso de una universidad pública mexicana. ***Revista Conrado, 18(84)***, 218-224.

RESUMEN

Las contraseñas basadas en texto son un mecanismo fundamental para proteger accesos y datos. Sin embargo, paradójicamente, las contraseñas débiles o mal utilizadas representan vulnerabilidades peligrosas para los sistemas informáticos y sus usuarios. Los objetivos de este trabajo fueron caracterizar y comparar la estructura y el uso de contraseñas entre estudiantes de tres programas académicos ofertados por una universidad estatal pública mexicana. Los participantes fueron 299 alumnos registrados en las carreras de Administración, Tecnologías de la Información y Contaduría Pública. El diseño de investigación fue cuantitativo, transversal y correlacional. Se aplicó un cuestionario, cuyas respuestas fueron introducidas al software SPSS. Se realizaron pruebas no paramétricas de Kruskal-Wallis y correlaciones de Spearman.

Palabras clave:

Sistemas de información, Formación, Enseñanza Superior.

ABSTRACT

Text-based passwords are a fundamental mechanism for protecting access and data. However, paradoxically, weak, or misused passwords represent dangerous vulnerabilities for computer systems and their users. The objectives of this study were to characterize and compare the structure and use of passwords among university students in three academic programs offered by a Mexican state university. The participants were 299 students enrolled in Administration, Information Technology, and Public Accounting undergraduate programs. The research design was quantitative, cross-sectional, and correlational. A questionnaire was administered. The collected answers were entered into SPSS software. Kruskal-Wallis and Spearman correlation tests were performed. Information

Keywords:

Information Systems, Training, Higher Education.

INTRODUCCIÓN.

La seguridad es un tema relevante para todos los usuarios de sistemas de información; en especial en la actualidad, cuando el número de dispositivos inteligentes ha superado la cifra de 4.2 billones en el año 2020 (Alzubaidi, 2021). Y es que el uso cotidiano de las redes de comunicación propicia serias vulnerabilidades.

Diariamente se conocen incidentes que violan la privacidad de personas y empresas, en muchas ocasiones con pérdidas cuantiosas. Parkinson, et al. (2021), destacan que en la sociedad moderna es necesario restringir accesos a los sistemas de información para que únicamente los usuarios autorizados puedan ingresar. Esto puede lograrse a través de la autenticación con contraseñas. Si bien es cierto que existen variados mecanismos para restringir accesos no autorizados, las contraseñas basadas en texto siguen siendo una manera popular de implementar estas restricciones (Yıldırım, & Mackie, 2019; Kim, et al., 2021).

Sin embargo, el solo hecho de contar con una contraseña no libera a los usuarios del peligro de las intrusiones. Una contraseña debe ser robusta. Es decir, debe poseer fuertes características estructurales como, por ejemplo, una longitud adecuada, una variedad de letras mayúsculas, minúsculas, números y caracteres especiales, así como la exclusión de datos fáciles de adivinar. Además, es una buena práctica cambiarlas frecuentemente. Para Buil-Gil, et al. (2020), las contraseñas robustas son una forma de protección personal, así como también lo son la concientización sobre riesgos digitales, evitar hacer transacciones con negocios y personas que no cumplen estándares de ciberseguridad y asistir a entrenamientos y seminarios sobre este tema.

En continuación a lo expuesto por Buil-Gil, et al. (2020), a pesar de que un sistema informático posea sofisticadas características de seguridad y contraseñas robustas, estas serían de poca utilidad si sus usuarios no cuentan con las actitudes y la formación apropiadas. Esto es porque los usuarios son el eslabón más débil en la cadena de mecanismos de protección (Peterson, 2017; Wiseman, 2017). Por esta razón, tanto las contraseñas débiles como las que son mal utilizadas por los usuarios representan peligros potenciales para cualquier sistema de información.

En este sentido, Stanciu, & Tinca (2016), consideran que el mejoramiento de la seguridad informática debe ser impulsado desde la universidad y no solo con una perspectiva tecnológica, como usualmente se hace, sino también con una acentuación específica por áreas de estudio. Esto porque además de la formación técnica de las personas, también son destacables su buena actitud y conducta en el contexto de la seguridad informática. Por su parte, Case & King (2013), encontraron cambios positivos en la seguridad informática de estudiantes universitarios, los cuales son atribuibles a la capacitación adicional que se impartió dentro de sus asignaturas regulares.

Por otra parte, Whitty, et al. (2015), encontraron que a pesar de que los usuarios conocen los lineamientos sobre el uso correcto de sus contraseñas, tienen la creencia de que ellos no sufrirán incidentes de seguridad. Entonces se revisten con una falsa certeza que los induce a realizar conductas arriesgadas. Asimismo, encontraron que los jóvenes tienen una mayor tendencia para compartir sus contraseñas y que son ellos, los jóvenes, quienes deben ser objeto de mayor capacitación y concientización en el área de la seguridad informática.

En este punto surge la importancia de la formación en seguridad informática. Los usuarios deben ser capaces de construir contraseñas robustas y deben, además, tener una buena conciencia sobre su uso.

El artículo está organizado de esta manera: en el siguiente apartado se muestra la descripción de la metodología del estudio, luego se presentan los resultados y su discusión. Finalmente se exponen las conclusiones y las líneas de trabajo futuro.

MATERIALES Y MÉTODOS

La población considerada para este estudio fueron los estudiantes que estaban registrados durante el periodo de primavera de 2020 en las siguientes tres carreras profesionales: licenciatura en administración, licenciatura en tecnologías de la información y contaduría pública de una universidad pública estatal mexicana. La muestra fue estadísticamente representativa y se obtuvo con la calculadora en línea disponible en Yıldırım & Mackie (2019). Se consideró un universo de 1350 estudiantes, una heterogeneidad del 50%, un nivel de confianza del 95% y un margen de error del 5%.

La muestra resultó en 299 estudiantes distribuidos en los tres programas educativos. La población y la muestra se describen en la Tabla 1.

Tabla 1. Descripción de la población y muestra.

Programa académico	Población	Muestra (Participantes)
Licenciatura en Tecnologías de la Información (LTI)	200	44
Licenciatura en Administración (LA)	640	144
Contaduría Pública (CP)	500	111
Total	1350	299

Se revisó la literatura y se procedió a diseñar un cuestionario pensando en acortar al mínimo el tiempo de respuesta de los participantes. La versión final fue refinada en dos revisiones en donde se realizaron adecuaciones en la redacción de las preguntas. El cuestionario fue reproducido en hojas de papel y fue entregado a los estudiantes seleccionados aleatoriamente del marco muestral de cada uno de los programas académicos. Los estudiantes fueron abordados en sus aulas, mientras tomaban clases presenciales justo antes del inicio de la contingencia sanitaria decretada a causa del COVID-19 en marzo de 2020. Posteriormente se procedió a la captura y análisis de los datos en SPSS versión 25. Finalmente, se obtuvieron los resultados y se realizaron reflexiones sobre ellos.

Instrumento de recolección de datos

Se utilizó un cuestionario con seis preguntas, las cuales se muestran en la tabla 2.

Tabla 2. Instrumento de recolección de datos.

Identificador	Pregunta	Escala de respuesta
P1	¿Qué tan probable es que en una contraseña usted incluya fechas importantes como cumpleaños o aniversarios?	0 a 10
P2	¿Qué tan probable es que usted comparta alguna contraseña con otra persona?	0 a 10
P3	¿De cuántos caracteres en total es la contraseña de la cuenta de correo electrónico que usted más utiliza?	1 a 20
P4	¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?	0 a 20
P5	¿Qué tan probable es que use la misma contraseña en dos o más páginas web?	0 a 10
P6	¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?	0 a 10

El análisis de datos se realizó en el paquete estadístico SPSS versión 25. Primero, se inspeccionaron los datos para encontrar valores perdidos, inválidos o mal capturados. Posteriormente se verificó si existía normalidad en cada uno de los grupos de respuestas de los programas académicos, para lo cual se aplicó la prueba de Shapiro-Wilk. Después se obtuvieron los estadísticos descriptivos que consistieron en la mediana y el rango intercuartil. Luego se procedió a realizar las pruebas no paramétricas Kruskal-Wallis y a analizar las comparaciones entre grupos para cada una de las preguntas que resultaron significativas. Finalmente se realizaron análisis de correlación de Spearman, los cuales involucraron las seis preguntas del cuestionario. En todos los casos se utilizó un nivel de confianza del 95%.

RESULTADOS Y DISCUSIÓN

En la Tabla 3 se muestran los resultados de la prueba de normalidad de Shapiro-Wilk. No se encontró distribución normal en ningún conjunto de respuestas analizado por programa académico. Por esta razón, se utilizó estadística no paramétrica para describir y comparar los datos. La mediana y el rango intercuartil de cada conjunto de respuestas se muestran en la Tabla 4.

Tabla 3. Valor p de la prueba de normalidad de Shapiro-Wilk.

	P1 ¿Qué tan probable es que en una contraseña usted incluya fechas importantes como cumpleaños o aniversarios?	P2 ¿Qué tan probable es que usted comparta alguna contraseña con otra persona?	P3 ¿De cuántos caracteres en total es la contraseña de la cuenta de correo electrónico que usted más utiliza?	P4 ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?	P5 ¿Qué tan probable es que use la misma contraseña en dos o más páginas web?	P6 ¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?
LTI	.00	.00	.027	.00	.00	.00
LA	.00	.00	.00	.00	.00	.00
CP	.00	.00	.00	.00	.00	.00

Tabla 4. Estadísticos descriptivos de los datos recabados. Los valores se muestran en el formato Mediana (Rango intercuartil).

	P1 ¿Qué tan probable es que en una contraseña usted incluya fechas importantes como cumpleaños o aniversarios?	P2 ¿Qué tan probable es que usted comparta alguna contraseña con otra persona?	P3 ¿De cuántos caracteres en total es la contraseña de la cuenta de correo electrónico que usted más utiliza?	P4 ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?	P5 ¿Qué tan probable es que use la misma contraseña en dos o más páginas web?	P6 ¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?
LTI	1 (6)	0 (4)	10 (6)	2 (6)	5 (8)	2 (6)
LA	2 (5)	1 (2)	10 (4)	0 (2)	5.50 (6)	0 (2)
CP	3 (7)	1 (2)	10 (4)	1 (3)	7 (8)	0 (3)

Las pruebas de Kruskal-Wallis que se llevaron a cabo para comparar las respuestas obtenidas en los tres programas académicos arrojaron los resultados que se muestran en la Tabla 5. Solamente se pudieron determinar diferencias estadísticamente significativas en las respuestas a la Pregunta 4 (P4) y a la Pregunta 6 (P6).

Tabla 5. Resultados de las pruebas Kruskal-Wallis para comparar los tres programas académicos.

	P1 ¿Qué tan probable es que en una contraseña usted incluya fechas importantes como cumpleaños o aniversarios?	P2 ¿Qué tan probable es que usted comparta alguna contraseña con otra persona?	P3 ¿De cuántos caracteres en total es la contraseña de la cuenta de correo electrónico que usted más utiliza?	P4 ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?	P5 ¿Qué tan probable es que use la misma contraseña en dos o más páginas web?	P6 ¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?
H	1.302	0.235	0.141	8.396	2.126	10.775
gl	2	2	2	2	2	2
Sig.	0.522	0.889	0.932	0.015*	0.345	0.005*

* $p < .05$

Una vez que se determinaron resultados significativos para las preguntas 4 y 6 (P4 y P6), se indagó en cuáles de los programas académicos se encontraban las diferencias. La Tabla 6 muestra los rangos promedio que se obtuvieron en las pruebas. Los rangos promedio más grandes indican la concentración de las puntuaciones más altas en ese programa académico. Por el contrario, las puntuaciones más bajas se ubicaron en los programas académicos con los rangos promedio más bajos.

Tabla 6. Rangos promedio para las pruebas Kruskal-Wallis con resultados estadísticamente significativos.

P4 ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?	
LTI	178.39
LA	138.83
CP	151.91
P6 ¿Que tan probable es que usted cambie la contraseña de su correo una vez al mes?	
LTI	185.94
LA	141.17
CP	145.83

La Figura 1 y la Figura 2 presentan de manera visual las relaciones entre los tres programas académicos analizados para la pregunta 4 (P4. ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo que usted más utiliza?) y la pregunta 6 (P6. ¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?) respectivamente. Las líneas en color amarillo representan relaciones estadísticamente significativas. Por otra parte, la Tabla 7 y la Tabla 8 muestran los detalles numéricos de las comparaciones entre los tres programas académicos. Cada fila prueba la hipótesis nula de que las distribuciones de la muestra 1 y la muestra 2 son las mismas. Las significaciones que se muestran son asintóticas bilaterales. Se utilizó un nivel de significación de .05 y los ajustes se realizaron mediante la corrección de Bonferroni para varias pruebas.

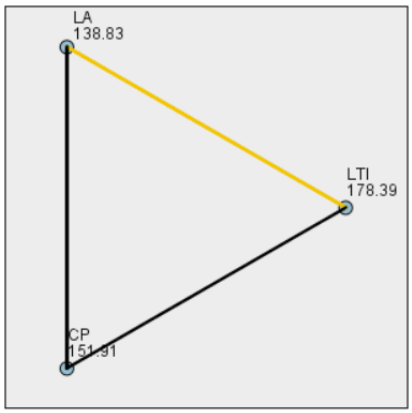

Figura 1. Comparaciones entre programas educativos. Se muestran los rangos promedio obtenidos en la prueba Kruskal-Wallis para la Pregunta P4.

Tabla 7. Comparación estadística de las respuestas a la pregunta P4 entre los programas académicos analizados.

Muestra 1 – Muestra 2	Estadístico de contraste	Sig.	Sig. Ajustada.
LA – CP	-13.084	.197	.590
LA -LTI	39.557	.004	.012*
CP - LTI	26.473	.064	.191

* $p < .05$

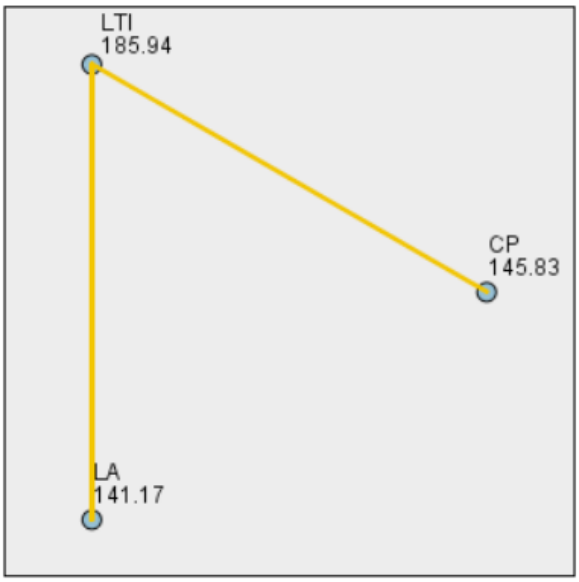

Figura 2. Comparaciones entre programas educativos. Se muestran los rangos promedio obtenidos en la prueba Kruskal-Wallis para la Pregunta P6.

Tabla 8. Comparación estadística de las respuestas a la pregunta P6 entre los programas académicos analizados.

Muestra 1 – Muestra 2	Estadístico de contraste	Sig.	Sig. Ajustada.
LA - CP	-4.657	.648	1.000
LA - LTI	44.773	.001	.004*
CP - LTI	40.116	.005	.016*

* $p < .05$

El análisis de correlación de Spearman que se realizó con las seis preguntas del cuestionario arrojó los resultados significativos que se muestran en la Tabla 9.

Tabla 9. Resultados significativos de las correlaciones de Spearman.

Programa académico	Aspecto analizado #1	Aspecto analizado #2	Coeficiente de correlación	Sig. (Bilateral)
Tecnologías de la información	Probabilidad de utilizar la misma contraseña en dos o más lugares (P5)	Probabilidad de compartir contraseñas con otra persona (P2)	0.29	0.05
		Probabilidad de incluir fechas en la contraseña (P1)	0.35	0.01
Administración	Probabilidad de utilizar la misma contraseña en dos o más lugares (P5)	Cantidad de caracteres especiales en la contraseña de la cuenta de correo más usada (P4)	-0.19	0.02
		Probabilidad de incluir fechas en la contraseña (P1)	0.20	0.01
	Cantidad de caracteres especiales en la contraseña de correo más usada (P4)	Probabilidad de cambiar la contraseña frecuentemente (P6)	0.30	0.00
Contaduría Pública	Probabilidad de utilizar la misma contraseña en dos o más lugares (P5)	Cantidad de caracteres especiales en la contraseña de la cuenta de correo más usada (P4)	-0.20	0.02
		Probabilidad de compartir contraseñas con otra persona (P2)	0.18	0.04
		Probabilidad de incluir fechas en la contraseña (P1)	0.30	0.00
	Probabilidad de compartir contraseñas con otra persona (P2)	Probabilidad de incluir fechas en la contraseña (P1)	0.33	0.00

Se considera que la longitud de las contraseñas es un factor importante para la seguridad que estas brindan. Así, una contraseña más grande es un indicador de mayor robustez (Yıldırım & Mackie, 2019). Siguiendo esta lógica, se encontró que los estudiantes de los tres programas académicos utilizan contraseñas de longitud similar. La cantidad media fue de diez caracteres en los tres programas académicos, lo cual se considera un buen indicador.

Por otra parte, el número de caracteres especiales es otro factor que incrementa la robustez de las contraseñas. En este sentido, se encontró que los alumnos de la Licenciatura en Tecnologías de la información utilizan contraseñas más seguras, pues incluyen mayor número de caracteres especiales que quienes estudian Administración o Contaduría Pública. Por su parte, los alumnos del programa educativo de Administración reportaron la menor cantidad de caracteres especiales en sus contraseñas.

A pesar de que las diferencias encontradas en la probabilidad reportada por los estudiantes para incluir datos sensibles como fechas en sus contraseñas no resultó estadísticamente significativa, se pudo observar a través de las medidas de tendencia central que los alumnos de la carrera de Tecnologías de la información son menos proclives a incluir fechas en sus contraseñas que los alumnos de las carreras de Administración y Contaduría Pública.

No se pudo establecer que las diferencias observadas en la probabilidad de compartir las contraseñas con otras personas fueran significativas. Sin embargo, en este sentido, se pudo observar que los alumnos de Tecnologías de la información reportaron una probabilidad inferior que los alumnos de los otros dos programas académicos.

El uso repetido de contraseñas en varios lugares no resultó diferente entre los tres programas académicos analizados. Sin embargo, tanto en Tecnologías de la información como en Administración y Contaduría Pública se observó una probabilidad de media a alta para reutilizar las contraseñas, lo cual es una práctica no recomendada y representa una importante área de mejora.

Se encontró que los estudiantes de Tecnologías de la información tienen mayor probabilidad de cambiar sus contraseñas más frecuentemente que los estudiantes del resto de los programas académicos. Aun así, la probabilidad reportada por los tres programas académicos es muy baja. Esto representa otra área que puede fortalecerse.

Sobre los hábitos y prácticas

Al buscar oportunidades de mejora en las prácticas de seguridad informática de los estudiantes, se encontró en los tres programas académicos que los alumnos con altas probabilidades de tener una mala práctica simultáneamente tienen altas probabilidades de tener otras malas prácticas con relación a sus contraseñas. Esto se acentúa en los programas de Contaduría Pública (CP) y Administración (LA). La Tabla 10 muestra estos detalles.

Tabla 10. Interpretación de las correlaciones analizadas.

Aspecto 1	Aspecto 2	Programa, sentido y fuerza de relación	Interpretación
P2 – Probabilidad de compartir contraseñas	P1 – Probabilidad de incluir fechas	CP (+)	A (mayor/menor) probabilidad de compartir contraseñas, (mayor/menor) probabilidad de incluir fechas.
P5 – Uso repetido de contraseñas	P1 – Probabilidad de incluir fechas	LTI (+) LA (+) CP (+)	A (mayor/menor) probabilidad de utilizar la contraseña en varios lugares, (mayor/menor) probabilidad de incluir fechas.
P5 – Uso repetido de contraseñas	P2 – Probabilidad de compartir contraseñas	LTI (+) CP (+)	A (mayor/menor) probabilidad de utilizar la contraseña en varios lugares, (mayor/menor) probabilidad de compartir la contraseña.
P5 – Uso repetido de contraseñas	P4 – Cantidad de caracteres especiales	LA (-) CP (-)	A (mayor/menor) probabilidad de utilizar la contraseña en varios lugares, (menor/mayor) cantidad de caracteres especiales en la contraseña.
P6 – Cambio frecuente	P4 – Cantidad de caracteres especiales	LA (+)	A (mayor/menor) cambio frecuente de contraseñas, (mayor/menor) cantidad de caracteres especiales.

Los resultados invitan a fortalecer la seguridad informática de los estudiantes desde el contexto universitario, considerando el perfil del programa educativo en el que se encuentran inscritos. En este sentido, coinciden con el trabajo de Stanciu & Tinca (2016). El caso del programa académico de Licenciatura en Tecnologías de la información, en donde se encontraron oportunidades de mejora en el área de seguridad informática, sugiere que los alumnos pueden tener

una conducta confiada y arriesgada, tal como lo sugieren Witty, et al. (2015). Por otra parte, las conclusiones de este trabajo son concordantes con los puntos de vista de Buil-Gil, et al. (2020), quienes consideran que tanto las contraseñas robustas como la concientización y entrenamientos en seguridad informática son elementos de protección personal.

Sobre las implicaciones prácticas de los resultados

Seguramente por la naturaleza misma de su carrera, los alumnos de Licenciatura en tecnologías de la información tienen contraseñas con mejores características, así como también reportan un mejor uso de estas. Sin embargo, también ellos podrían mejorar su nivel de seguridad informática. Por ejemplo, al reutilizar menos las contraseñas y cambiarlas más frecuentemente. Los alumnos de Administración y de Contaduría Pública, además de estos aspectos, podrían compartir menos sus contraseñas, robustecerlas con mayor número de caracteres especiales, o no incluir en ellas fechas que resulten fáciles de adivinar. Por otra parte, los resultados sugieren que los alumnos suelen tener simultáneamente varias prácticas poco recomendables en el área de seguridad informática. Por estas razones, es evidente la necesidad de fortalecer la seguridad informática en los tres programas analizados.

El estudio, por ejemplo, se realizó en una sola universidad mexicana y el instrumento utilizado permitió estudiar un reducido número de aspectos. Por otra parte, el análisis de datos excluyó los datos demográficos como edad, semestre y género y estuvo centrado en el análisis por programa educativo. Por otra parte, el alcance del trabajo se ubicó en los niveles descriptivo y relacional.

Como trabajo futuro se plantea superar las limitaciones de la investigación a través del estudio descriptivo y comparativo de estas y otras facetas relacionadas con las contraseñas, especialmente durante la época de contingencia sanitaria por COVID-19, ya que los sistemas informáticos adquirieron una renovada relevancia a causa del confinamiento y el teletrabajo.

CONCLUSIONES

Las contraseñas robustas y su buen uso son factores necesarios para fortalecer los niveles de seguridad informática.

Los estudiantes universitarios pueden mejorar tanto la estructura como el uso de sus contraseñas. Si bien los alumnos de tecnologías de la información mostraron una ventaja en este sentido sobre quienes cursan los programas académicos de administración y contaduría pública, todos son susceptibles de mejorar sus niveles de seguridad. Esto puede lograrse a través de la capacitación y la concientización orientadas a la luz de las necesidades de los estudiantes.

A pesar de que se detectaron áreas de mejora en todos los programas académicos, los alumnos de Tecnologías de la Información resultaron los menos vulnerables. Por otra parte, los estudiantes de Administración fueron los más vulnerables.

REFERENCIAS BIBLIOGRÁFICAS

Alzubaidi, A. (2021). Medición del nivel de concientización en materia de ciberseguridad para la ciberdelincuencia en Arabia Saudí. ***Heliyon***, ***7(1).***

Buil-Gil, D., Lord, N., & Barrett, E. (2020). La dinámica de las empresas, la ciberseguridad y la cibervictimización: El protagonismo del guardián interno en la prevención. ***Victims & Offenders***, ***16(3),*** 286–315.

Case, C. J., & King, D. L. (2013). Ciberseguridad: Un examen longitudinal del comportamiento y las percepciones de los estudiantes. ***ASBBS EJournal***, ***9(1),*** 21–29.

Kim, P., Lee, Y., Hong, Y. S., & Kwon, T. (2021). Un medidor de contraseñas sin exposición de contraseñas. ***Sensors (Switzerland)***, ***21(2),*** 1–25.

Parkinson, S., Khan, S., Crampton, A., Xu, Q., Xie, W., Liu, N., & Dakin, K. (2021). Password policy characteristics and keystroke biometric authentication. ***IET Biometrics***, 10***(2),*** 163–178.

Peterson, A. H. (2017). Un empleado negligente. ***Credit Union Magazine***, ***9***, 10–10.

Stanciu, V., & Tinca, A. (2016). La sensibilización de los estudiantes sobre la seguridad de la información entre la propia percepción y la realidad-un estudio empírico. ***Accounting and Management Information Systems***, ***15(1),*** 112–130.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Diferencias individuales en los comportamientos de ciberseguridad: Un análisis de quién comparte las contraseñas]. ***Cyberpsychology, Behavior, and Social Networking, 18(1),*** 3–7.

Wiseman, C. (2017). Ciberseguridad de la empresa de contabilidad: Formación de su personal y protección de su empresa]. ***CPA Practice Advisor***, ***1***, 27–27.

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. ***International Journal of Information Security***, ***18(6),*** 741–759.